APPENDIX E

DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII)

Policy

1. The Defense Clearance and Investigations Index (DCII) is the single, automated central repository that identifies investigations conducted by Department of Defense (DoD) investigative agencies. The DCII also includes data on personnel security determinations made by DoD adjudicative authorities.

2. The data base consists of social security number and alphanumeric index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects in investigative documents maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are indexed alphabetically by subject and numerically by social security number.

Access to the DCII

1. The DCII is operated and maintained by the Defense Security Service (DSS). Access is normally limited to the DoD and other Federal Agencies with adjudicative, investigative and/or counterintelligence missions.

2. Access to a DCII terminal will be from the DSS mainframe computer to a web version. Smartgate Tokens are required on hardware to pass through the DSS firewall to access the DCII system.

3. Commands desiring to gain access to the DCII must submit a written request outlining the justification and specific requirements for **query** "Read-Only" access to the DCII. The request must be submitted via CNO (N09N2) for approval and endorsement to the Chief, Office of Congressional and Public Affairs, Defense Security Service, (V0105).

4. Upon approval by DSS, a Memorandum of Understanding (MOU) addressing equipment, maintenance, security, privacy, and other command responsibilities will be forwarded directly to the command from DSS.

Security Requirements for the DCII

1. The DCII is an unclassified system that meets the C-2 level of protection under the Computer Security Act of 1987.

2. The information contained in the DCII receives the same protection required by the Privacy Act of 1974.

3. Due to the sensitive nature of the information contained in the database, positions for individuals having direct (password) access to a DCII terminal must have a favorably completed NAC/NACI for "read only" access to the DCII and a favorably completed SSBI/PR is required for those individuals who input into the DCII.

4. To prevent unauthorized access or tampering during nonworking hours, DCII terminals must be located in an area that is secured by guard personnel, an alarm system, or appropriate locking device.

5. When the DCII terminal is operational, access to DCII information shall be controlled and limited to those persons authorized access to that information.